REMARKS

Status of Claims

Claims 1-4, 7-10, 12-13, 18-22, 24-28 and 33-34 are pending in the present application, with claims 1, 12, 22, 26, and 33 being the independent claims. Claims 1, 12, 22, 26-28, and 33-34 have been amended to address the wording objections and the rejections under 35 U.S.C. §112, first and second paragraphs. Claim 14 has been canceled. No claim has been added. No new matter has been entered.

Interview Summary

Telephonic interviews were conducted between Applicant's undersigned representative and Examiner Dinh on February 12-13, 2008, to discuss the rejections in the Official Action mailed November 21, 2007. Applicant presented a draft amendment response with proposed amendments for overcoming the rejections under 35 U.S.C. §112, first and second paragraphs, and the proposed amendments to the claims were discussed during the interviews. The above amendments incorporate the changes proposed during the interviews as well as additional changes to claims 1, 12, 22, and 26 based on Examiner Dinh's comments during the interviews. Applicant now further proposes to cancel claim 14 due to the additional amendments to claim 12 and to amend claims 27-28 for consistency with amended claim 26 and to amend claim 34 for consistency with amended claim 33. The amendments to claims 12 and 22 bring these claims more in line with claim 1, which Examiner Dinh indicated to be generally acceptable pending more careful review once the present amendment response is formally filed. Examiner Dinh also indicated that the proposed amendments to claim 33 are generally acceptable pending more careful review once the present amendment response is filed. Examiner Dinh also requested that claim 26 be amended to recite steps, which Applicant has now done in the proposed amendments to claim 26.

The following will act as a summary of the interview. Examiner Dinh is encouraged to contact Applicant's undersigned representative to discuss any further amendments that may facilitate allowance of the present application.

Claim Objections

Claims 1-4, 7-10, 12-14, 18-22, and 24-25 stand objected to because of informalities in the antecedent basis of "callback access control entry" in independent claims 1, 12, and 22. Claims 1, 12, and 22 have been amended as recommended by the examiner in order to obviate the claim objections. Withdrawal of the objections to claims 1-4, 7-10, 12-14, 18-22, and 24-25 is solicited.

Rejection under 35 U.S.C. § 112, First Paragraph – Claims 26-28

Claims 26-28 stand rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement by reciting in claim 26 that "said dynamic groups element and a dynamic access element utilize dynamic data that includes authorization policy data stored in a callback access control entry and/or run-time data managed by the application." Claims 26-28 have been amended to obviate the rejection by removing from claim 26 the language specifying that the authorization policy data is "stored in callback access control entry" and moving such language to dependent claim 28. The amended language of claim 26 now tracks the description of Figures 5A-5C and the text at page 4, line 24, through page 6, line 2, and at page16, line 19, through page 19, line 10, of the specification. Given that the language of claims 26-28 is clearly described in the recited portions of the specification, the recited language is believed to be specifically supported in the originally filed specification. Reconsideration and withdrawal of the rejection of claims 26-28 based on 35 U.S.C. § 112, first paragraph, is solicited.

Rejection under 35 U.S.C. § 112, First Paragraph – Claims 33-34

Claims 33-34 stand rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement by allegedly failing to disclose invoking a dynamic access check callback function to "initialize a client authorization context from a system level authorization context or a user's security identifier," or that "the client context is augmented with client contextual data dynamically computed using said dynamic data." The objectionable language has been removed from claim 33 so as to obviate this rejection. Claim 33 now recites "when a user attempts to connect to the application, automatically invoking a registered dynamic access check callback function to provide said customized procedures for checking access rights based on said transient or changing factors" as clearly described in the specification with respect to Figures 5A-5C (*e.g.*, see step 560 in

Figure 5A and page 4, line 24, through page 6, line 2, of the specification). Claim 34 has been amended for consistency with claim 33. In view of these amendments, reconsideration and withdrawal of the rejection of claims 33-34 based on 35 U.S.C. § 112, first paragraph, is solicited.

Rejection under 35 U.S.C. § 112, Second Paragraph - Claims 1-4, 7-10, 12-14, 18-22, and 24-25

Claims 1-4, 7-10, 12-14, 18-22, and 24-25 stand rejected under 35 U.S.C. § 112, second paragraph, as allegedly being incomplete for omitting "essential steps." Applicant has amended independent claims 1, 12, and 22 to better track each other as well as the steps of Figures 5A-5C. In view of Examiner Dinh's indication that claim 1 is generally acceptable, the corresponding amendments to claims 12 and 22 are believed to overcome Examiner Dinh's objections to claims 12 and 22 as well. If this is not the case, Examiner Dinh is encouraged to contact Applicant's undersigned representative to discuss appropriate claim amendments to overcome all remaining objections to the claims. Withdrawal of the rejection of claims 1-4, 7-10, 12-14, 18-22, and 24-25 based on 35 U.S.C. § 112, second paragraph, is solicited.

Rejection under 35 U.S.C. § 112, Second Paragraph - Claims 1-4, 7-10, 12-14, and 18-21

Claims 1-4, 7-10, 12-14, 18-22, and 24-25 also stand rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for inconsistent antecedent references to "dynamic data." Independent claims 1 and 12 have been amended to clear up antecedent basis. Withdrawal of the rejection of claims 1-4, 7-10, 12-14, and 18-21 based on 35 U.S.C. § 112, second paragraph, is solicited.

Rejection under 35 U.S.C. § 102(e) – Claims 1-10 and 12-29

Claims 1-4, 7-10. 12-14. 18-22, and 24-28 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Swift (USP 6,308,274). Claims 1, 12, 22, and 26 have been amended to obviate this rejection. The distinctions between the claimed methods and computer readable media and Swift will be described below.

Independent claim 1 has been amended to recite:

> initializing a client authorization context for the client using one or more client context initialization routines;
> determining, via an application programming interface, based upon dynamic data possessed by the application and a first dynamic policy whether

> said client authorization context is to be updated and, if so, updating said client authorization context, wherein said first dynamic policy is tailored to said application;
>
> invoking an access check routine to determine if the application or client represented by the client authorization context is allowed access to the resource, the application providing said dynamic data and an identifier for the access check to the access check routine for comparison against access control entries;
>
> identifying an access control entry as a callback access control entry; and
>
> in response to identifying the access control entry as a callback access control entry and a match between said identifier and an identifier in the callback access control entry, automatically invoking, via said application programming interface, an application-defined dynamic access check routine that performs the access check for the application based upon said dynamic data and a second dynamic policy in the callback access control entry for the application, wherein said second dynamic policy is tailored to said application and said dynamic data includes authorization policy data stored in said callback access control entry and/or run-time data managed by the application.

Thus, the client authorization context and the access check routine are modified based on dynamic data and dynamic policies that are tailored to the application requesting the resource, where the "dynamic data includes authorization policy data stored in said callback access control entry and/or run-time data managed by the application." Similar limitations may be found in independent claims 12 and 22. Also, claim 26 further recites:

> carrying out a dynamic authorization callback mechanism to determine if the application or client represented by the updated client authorization context is allowed access to the resource, the dynamic authorization callback mechanism providing extensible support for application-defined business rules via a set of APIs and DACLs including a dynamic groups element, and said dynamic groups element enabling said application to assign temporary group membership, based on dynamic factors, to said client for the purpose of checking access rights, wherein said dynamic groups element and a dynamic access element utilize dynamic data that includes authorization policy data and/or run-time data managed by the application.

Such features are not taught by Swift.

As discussed during the interview on February 12, 2008, Swift provides restricted access tokens to enforce least privilege. The restricted token is based on an existing token and has less access rights than the existing token. For example, the restricted token may have a changed attribute of one or more security identifiers that denies access in the restricted token where access was permitted in the existing token. The process to be restricted is associated with the restricted token. However, Swift nowhere describes modifying an existing token to update the client authorization context and to invoke an "application-defined dynamic access check routine" based on "dynamic data" as claimed. Applicant submits that Swift's teaching of removing one or more privileges in a restricted token is not a teaching of modifying the client authorization context based on "dynamic data" and "dynamic policies" as claimed. As recited in independent claims 1, 12, 22, and 26, the "dynamic data" includes "authorization policy data and/or run-time data managed by the application." Independent claim 33 further recites that the claimed "dynamic data" may comprise "an identifier for identifying whether a dynamic access check callback function should be invoked for conducting said dynamic authorization of said application, data from client operation parameters, authorization policy data stored in a callback access control entry, and any other authorization policy data managed, computed or retrieved by the application." Swift does not modify the token privileges based on such "dynamic data."

As noted in previous responses, while the restricted token based system of Swift is made more versatile by allowing the creation of restricted access tokens, Swift remains an example of a system that enforces static access policy in that every time a token, *e.g.*, a restricted token, of Swift is evaluated to determine whether a particular task can be performed by a user, or whether an application may access a particular object, *the token or restricted token is evaluated using static data with static access policies*. In particular, Swift enforces a static access policy, as described in the background section of Applicants' specification (See pages 1-2, first three paragraphs of background and page 13, lines 1-16). Swift says nothing of dynamically varying access policies for a particular application or changing a restricted token based on dynamic data. On the contrary, different restricted tokens are associated with *different* processes and do not provide for dynamic access policies regarding a particular application as claimed. The restricted tokens change only if the requesting process changes (and the new requesting process has a different associated restricted token) – the restricted tokens themselves are NOT generated for the same application according to dynamic factors. Restricted tokens as taught by Swift thus do not vary a client authorization context based on dynamic policies and/or dynamic data for a particular application as claimed.

In the "Response to Arguments" portion of the Official Action, the examiner has argued that the restricted SID taught by Swift corresponds to the claimed "dynamic data" and that the restricted token is "run-time data managed by the application." Applicant submits that there is no basis for the argument by the examiner that a restricted SID corresponds to "authorization policy data and/or run-time data managed by the application" as claimed. On the contrary, as described with respect to Figure 3 of Swift, the restricted SIDs are placed in a special field 92 of the restricted token 84 by the application based on the desired access rights and privileges for known processes and user groups (column 7, lines 50-61). No "authorization policy data" is provided in the SIDs. Moreover, the SIDs are not "run-time data managed by the application." Applicant can find no teaching in Swift that the restricted token is modified by the application during run-time. On the contrary, the SIDs are used only to deny access and cannot be used to grant access and *cannot later be removed or enabled*" (column 9, lines 56-59, emphasis added). In other words, as in the prior art access systems, the *token or restricted token in Swift is evaluated using static data with static access policies*. Also, unlike the claimed methods, access to the resource is NOT controlled based on "authorization policy data stored in a callback access control entry and/or run-time data managed by the application" as now claimed in claims 1, 12, and 22. Applicant again submits that Swift does not anticipate the use of dynamic data and dynamic policies as claimed. Swift further fails to teach that the dynamic data is used to enable the application "to assign temporary group membership, based on dynamic factors, to said client for the purpose of checking access rights" as claimed in claim 26.

Accordingly, the system of Swift is based on static policy and data and not the dynamic policy and data identified with specificity in the claims. Swift thus cannot be said to teach or suggest the methods and media as set forth in independent claims 1, 12, 22, and 26 and, through dependency, claims 2-4, 7-10, 13, 18-21, 24-25, and 27-28. Reconsideration and withdrawal of the §102(e) rejection based on Swift is respectfully requested.

Allowable Subject Matter – Claims 33-34

Applicant appreciates the Examiner's indication that claims 33-34 include allowable subject matter. In view of the amendments to these claims to address the §112, first paragraph, rejection of claim 33, claims 33-34 are now believed to be in condition for allowance.

Conclusion

Applicants believe that the present Amendment is responsive to each of the points raised by the Examiner in the Official Action, and submits that claims 1-4, 7-10, 12-13, 18-22, 24-28 and 33-34 of the application are in condition for allowance. Favorable consideration and issuance of a Notice of Allowability are earnestly solicited.

Date: February 21, 2008

/Michael P. Dunnam/
Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439